ABSTRACT

A method and apparatus for image compression using temporal and resolution layering of compressed image frames, and which provides encryption and watermarking capabilities. In particular, layered compression allows a form of modularized decomposition of an image that supports flexible encryption and watermarking techniques. Using layered compression, the base layer and various internal components of the base layer can be used to encrypt a compressed layered movie data stream. By using such a layered subset of the bits, the entire picture stream can be made unrecognizable by encrypting only a small fraction of the bits of the entire stream. A variety of encryption algorithms and strengths can be applied to various portions of the layered stream, including enhancement layers. Encryption algorithms or keys can be changed at each slice boundary as well, to provide greater intertwining of the encryption and the picture stream. Watermarking tracks lost or stolen copies back to the source, so that the nature of the method of theft can be determined and so that those involved in a theft can be identified. Watermarking preferably uses low order bits in certain coefficients in certain frames of a layered compression movie stream to provide reliable identification while being invisible or nearly invisible to the eye. An enhancement layer can also have its own unique identifying watermark structure.